Семинар 7. Квантовые вычисления

7.1 Введение

Из предыдущего изложения ясно, что необходимость построения квантового компьютера и разработка схемы квантовых вычислений возникает по двум причинам. Первая причина — технологическая. Фактическое развитие полупроводниковых технологий и технологий изготовления больших интегральных схем неизбежно приводит к тому, что для записи бита классической информации требуются все более и более микроскопические объекты приходя по существу к отдельным атомам и молекулам. Поведение этих объектов уже не укладывается в рамки классического описания и потому приходится либо считать, что достигнут технологический предел миниатюризации, либо решать проблему организации вычислений на квантовых объектах.

Вторая причина, которая стимулирует исследования в области квантовых компьютеров — это проявляющиеся принципиальные ограничения, которые возникают при использовании классических компьютеров, когда речь идет о возрастающем числе данных и экспоненциальном росте времени вычисления для многих, практически интересных и важных классических алгоритмов. Среди этих примеров приводится задача факторизации числа N на простые множители. В классической теории вычислений "приемлемыми" рассматриваются такие алгоритмы вычислений, в которых число шагов растет как полином небольшой степени от размера входных данных (например, полином второй или третьей степени).

Для задачи факторизации входными данными является число N, которое необходимо разложить на множители. Поэтому "длина" входных данных на классическом "двоичном" компьютере есть $\log_2 N$. Основание 2 логарифма связано с использованием двоичной системы исчисления. Известно, что лучшие алгоритмы факторизации выполняются за число шагов, k, которое имеет следующий порядок [1]

$$k = Const \cdot \exp\left\{(64/9)^{1/3}(\ln N)^{1/3}(\ln\ln N)^{2/3}\right\}. \qquad (7.1)$$

То есть алгоритм вычислений приводит к экспоненциальному росту числа шагов по мере роста числа входных данных. Так в 1994 году 129-значное число было факторизовано на 1600 рабочих станциях, распределенных по всему миру [2]. Время факторизации составило 8 месяцев. Используя результаты этого эксперимента можно качественно оценить порядок величины $Const$ в (7.1). Оценка числа времени, которое потребуется для факторизации 250-значного числа на тех же 1600 рабочих станциях дает $\sim 10^6$ лет (миллион лет!). Соответственно для факторизации 1000-значного числа потребуется 10^{25} лет, что на $11-12$ порядков больше (триллион лет) возраста вселенной, который оценивается в $10^{12}-10^{13}$ лет.

Сама по себе абстрактная задача факторизации очень больших чисел, помимо академического (считай никому не нужного) интереса имеет прямое отношение к системам криптографии с открытым ключом, нашедшим широкое применение в банковских системах. Забегая вперед, можно сказать, что факторизация 1000-значного числа с помощью квантового алгоритма потребует всего лишь несколько миллионов шагов и, следовательно, если квантовые алгоритмы удастся реализовать в реальном устройстве, то криптосистемы

[1] A.M. Odiyzko. AT&T Bell Laboratories, preprint 1995.

[2] S.L. Branstein. Encyclopedia of Applied Physics, Update, WILEY-VCH, 1999.

с открытым ключом, основанные на сложности факторизации чисел с приблизительно 250 знаками будут взломаны. Но естественно, не только задача "продажи" секретов банковским мошенникам стоит перед квантовыми вычислениями. Принципиальным фактом развития квантовых вычислений является возможность осуществления параллелизма в квантовых вычислениях, принципиально не доступного в классических устройствах.

7.2 Логические однокубитовые гейты

Классические компьютерные цепи состоят из проводов и набора логических гейтов (совокупности транзисторов). Провода служат для передачи стандартных напряжений по электрическим цепям, а логические гейты осуществляют преобразование "проходящей" через них информации. При этом единственным не тривиальным логическим гейтом, который преобразует 1 бит классической информации является NOT-гейт, действие которого сводится к преобразованиям битов вида: $0 \to 1$ и $1 \to 0$.

Одиночный кубит, по определению, является суперпозицией двух квантовых состояний $|0\rangle$ и $|1\rangle$, каждое из которых может рассматриваться как носитель одного бита классической информации

$$|\psi\rangle = a\ |0\rangle + b\ |1\rangle\,. \tag{7.2}$$

В соответствии с определением классического NOT-гейта, квантовый NOT-гейт (т.е. гейт преобразующий информацию внутри кубита) может быть определен по аналогии:

$$NOT:\ |\psi\rangle \to NOT:\ (a\ |0\rangle + b\ |1\rangle) \to a\ |1\rangle + b\ |0\rangle\,. \tag{7.3}$$

На основании теории представлений, квантовому состоянию кубита $|\psi\rangle$ (7.2) соответствует столбец

$$|\psi\rangle\ \to \begin{pmatrix} a \\ b \end{pmatrix}. \tag{7.4}$$

Поэтому квантовым аналогом классического NOT-гейта является матрица вида:

$$x \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad x\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}, \tag{7.5}$$

которая совпадает с матрицей Паули σ_x в s_z-представлении.

В соответствии с (7.4) квантовые гейты, преобразующие однокубитовое состояние являются унитарными матрицами размерности 2×2. В отличие от классических систем, для кубита можно построить неограниченное число гейтов. Однако, в силу полноты системы матриц Паули и единичной матрицы I, любая 2×2 матрица может быть разложена по этой полной системе матриц. Поэтому для практического использования представляют интерес сами матрицы Паули $X \equiv \sigma_x$, $Y \equiv \sigma_y$, $Z \equiv \sigma_z$ и некоторые их специальные комбинации, среди которых выделим следующие три:

$$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; \qquad S \equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}; \qquad T \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \tag{7.6}$$

Матрицы (7.6) определяют соответственно $H-$гейт Адамара, $S-$фазовый гейт, а T называется $\pi/8$-гейт. Из определения перечисленных гейтов следует, что:

$$H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) \equiv \frac{1}{\sqrt{2}}(X + Z); \qquad S = T^2. \tag{7.7}$$

Название T-гейта ($\pi/8$-гейт) определяется историческими причинами и возможностью представления матрицы этого гейта с точностью до общего фазового множителя $\exp(i\pi/8)$ в виде:

$$T \equiv \exp(i\pi/8)\begin{pmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{pmatrix} \tag{7.8}$$

Гейт Адамара является одним из наиболее полезных квантовых гейтов. Этот гейт иногда определяют как "квадратный корень от NOTгейт. Это связано с тем, что данный гейт преобразует $a\ |0\rangle$-часть кубита в $(|0\rangle + |1\rangle)/\sqrt{2}-$"половина пути" между $|0\rangle$ и $|1\rangle$ состояниями в геометрической интерпретации кубита на сфере Блоха. Соответственно в $|1\rangle$-части кубита преобразуется гейтом Адамара в комбинацию $(|0\rangle - |1\rangle)/\sqrt{2}$, что также "половина пути" между $|0\rangle$ и $|1\rangle$. Однако H^2-гейт не приводит к NOT-гейту, так как алгебраические вычисления дают $H^2 \equiv I$. То есть двухкратное применение гейта H возвращает систему в исходное положение.

Графическое обозначение однокубитовых гейтов представляют в виде:

$$\begin{aligned}
&a\,|0\rangle + b\,|1\rangle \text{ —— [X] —— } b\,|0\rangle + a\,|1\rangle \\
&a\,|0\rangle + b\,|1\rangle \text{ —— [Y] —— } -i\{b\,|0\rangle - a\,|1\rangle\} \\
&a\,|0\rangle + b\,|1\rangle \text{ —— [Z] —— } a\,|0\rangle - b\,|1\rangle \\
&a\,|0\rangle + b\,|1\rangle \text{ —— [H] —— } a\,\frac{|0\rangle + |1\rangle}{\sqrt{2}} + b\,\frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&a\,|0\rangle + b\,|1\rangle \text{ —— [S] —— } a\,|0\rangle + ib\,|1\rangle \\
&a\,|0\rangle + b\,|1\rangle \text{ —— [T] —— } a\,|0\rangle + e^{i\pi/4}b\,|1\rangle = \\
&\qquad = e^{i\pi/8}\{e^{-i\pi/8}a\,|0\rangle + e^{i\pi/8}b\,|1\rangle\}
\end{aligned} \tag{7.9}$$

Произвольный однокубитовый унитарный оператор может быть записан в виде:

$$U = \exp(i\alpha)\,R_{\vec{n}}(\theta), \tag{7.10}$$

где $R_{\vec{n}}(\theta)-$ оператор поворота на угол θ вокруг оси, определенной единичным вектором $\vec{n}$, α и $\theta-$ действительные числа.

Используя вид оператора поворота можно установить, что $T \equiv R_z(\pi/4)$, а гейт Адамара с точностью до глобального фазового множителя, является произведением операторов поворота R_x и R_z. С учетом условия антикоммутации матриц Паули $\sigma_x\sigma_y = -\sigma_y\sigma_x$ можно установить, что

$$X\,R_y(\theta)\,X = R_y(-\theta). \tag{7.11}$$

В алгебре матриц Паули доказывается теорема, которая называется **теоремой $X-Y$ разложения** для однокубитового гейта (или оператора). Содержание теоремы утверждает, что существуют действительные числа α, β, γ, δ такие, что унитарный оператор U может быть представлен в виде:

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta). \tag{7.12}$$

Обобщение этой теоремы может быть выполнено для двух произвольных направлений, определенных векторами $\vec{m}$ и $\vec{n}$. В этом случае однокубитовая унитарная матрица может быть записана в виде

$$U = e^{i\alpha} R_n(\beta_1) R_m(\gamma_1) R_n(\beta_2) R_m(\gamma_1) \dots \tag{7.13}$$

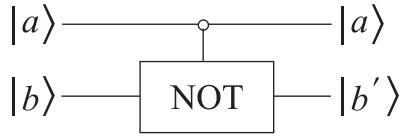
Для дальнейшего (с целью изучения квантовых цепей) полезно отметить следующие равенства

$$HXH = Z; \quad HYH = -Y; \quad HZH = X; \quad HTH = e^{i\alpha} R_x(\pi/4) \tag{7.14}$$

7.3 Контролируемые квантовые гейты

Простейшим двухкубитовым контролируемым гейтом в классическом компьютере является CNOT-гейт. В квантовых вычислениях водится, по сути подобный, гейт, который имеет два входных кубита и два кубита на выходе. Как и в классическом случае один из пары кубитов называется контролирующим, а второй контролируемым или кубитом-мишенью. Буквенное обозначение CNOT-квантового гейта не отличается от классического. Логика выполнения операции при этом определяется следующим образом: если контролирующий кубит находится в состоянии $|1\rangle$, тогда контролируемый кубит подвергается квантовой операции NOT, в противном случае контролируемый кубит остается без изменения. Графически "цепь" квантового CNOT-гейта изображается в виде:

$CNOT =$



(7.15)

Для пары кубитов $|a\rangle$ и $|b\rangle$ в качестве базисных можно выбрать вектора, являющиеся прямым произведением базисных векторов отдельных кубитов:

$$|0_a 0_b\rangle = |0_a\rangle \otimes |0_b\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \equiv \begin{pmatrix}1\\0\\0\\0\end{pmatrix}. \tag{7.16}$$

Аналогично оставшиеся 3 базисных состояния имеют вид:

$$|0_a 1_b\rangle \equiv \begin{pmatrix}0\\1\\0\\0\end{pmatrix}; \quad |1_a 0_b\rangle \equiv \begin{pmatrix}0\\0\\1\\0\end{pmatrix}; \quad |1_a 1_b\rangle \equiv \begin{pmatrix}0\\0\\0\\1\end{pmatrix}. \tag{7.17}$$

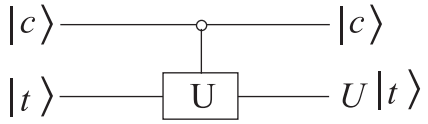
Чистое двухкубитовое квантовое состояние такой системы в общем виде определяется суперпозицией двухкубитовых базисных состояний

$$|\psi_{ab}\rangle = \alpha\,|0_a 0_b\rangle + \beta\,|0_a 1_b\rangle + \gamma\,|1_a 0_b\rangle + \delta\,|1_a 1_b\rangle \equiv \begin{pmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{pmatrix}. \tag{7.18}$$

Таким образом матрица квантового CNOT-гейт имеет следующий вид в базисе кубитов $|0\rangle$ и $|1\rangle$

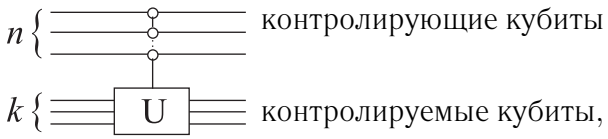
$$CNOT = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \tag{7.19}$$

Если выбирать в качестве оператора некоторый произвольный унитарный оператор, действующий на одиночный кубит, то контролируемая U-операция или CONTROLLED U-гейт можно графически определить следующим образом



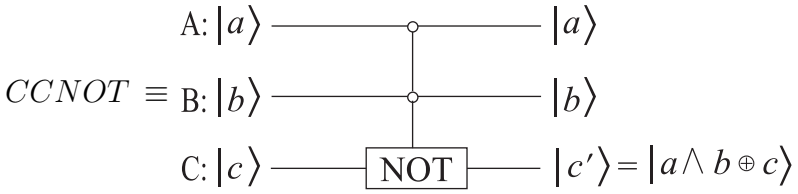
(7.20)

И в более общем случае



(7.21)

наиболее важным из которых является Тоффоли гейт или CCNOT-гейт



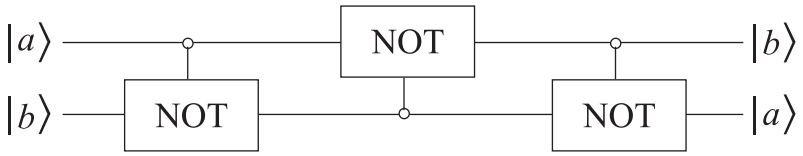
В этом гейте управляющими являются кубиты A и B, а $C-$ является управляемым. В пространстве базисных состояний 3-х кубитов $|0,0,0\rangle$, $|0,0,1\rangle$, $|0,1,0\rangle$, $|1,0,0\rangle$, $|1,0,1\rangle$,

$|1,1,0\rangle$, $|1,1,1\rangle$ он описывается следующей матрицей размерности 8×8

$$CCNOT \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

В теории квантовых вычислений доказывается утверждение о том, что однокубитовые гейты и CNOT-гейт являются универсальными.

Из многочисленных связок гейтов могут быть образованы произвольные квантовые "цепи", например

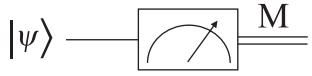


(7.22)

Последовательность преобразования кубитов в основном базисе выглядит здесь следующим образом:

$$\begin{aligned} |a,\, b\rangle &\rightarrow |a,\, a \oplus b\rangle \\ &\rightarrow |a \oplus (a \oplus b),\, a \oplus b\rangle = |b,\, a \oplus b\rangle \\ &\rightarrow |b,\, (a \oplus b) \oplus b\rangle = |b,\, a\rangle \end{aligned} \tag{7.23}$$

Важной операцией для кубитов является его измерение, которая отображается на рисунке символом:



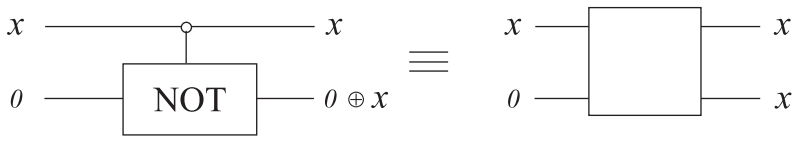
(7.24)

Операция измерение преобразует состояние одного кубита $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ в вероятностный классический бит M (изображаемый на выходе двойной линией), который может быть 0 с вероятностью $|a|^2$ или 1 с вероятностью $|b|^2$.

7.4 Невозможность клонирования кубита

CNOT-гейт позволяет продемонстрировать одно фундаментальное свойство квантовой информации. Как известно, задача копирования классического бита информации может быть

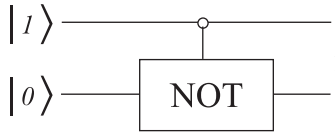
выполнена с использованием классического CNOT-гейта



(7.25)

В квантовом случае для произвольного кубита $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ имеем

вход $\equiv |\psi\rangle\,|0\rangle$:



выход : $a\,|00\rangle + b\,|11\rangle$ (7.26)

Начальное двухкубитовое состояние, которое подается на вход гейта CNOT имеет вид:

$$|\psi\rangle\,|0\rangle = \{a\,|0\rangle + b\,|1\rangle\}\,|0\rangle = a\,|0\rangle\,|0\rangle + b\,|1\rangle\,|0\rangle = a\,|00\rangle + b\,|10\rangle\,. \tag{7.27}$$

Так как гейт CNOT не преобразует состояние контролируемого кубита $|0\rangle$, если состояние контролирующего $|0\rangle$, и переворачивает состояние контролируемого кубита, при значении контролирующего $|1\rangle$, то очевидно:

$$\begin{aligned} CNOT &: a\,|00\rangle \;\rightarrow\; a\,|00\rangle \\ CNOT &: b\,|10\rangle \;\rightarrow\; b\,|11\rangle\,. \end{aligned}$$

Таким образом

$$CNOT\;:\;|\psi\rangle\,|0\rangle = |\psi, 0\rangle \;\rightarrow\; a\,|00\rangle + b\,|11\rangle\,. \tag{7.28}$$

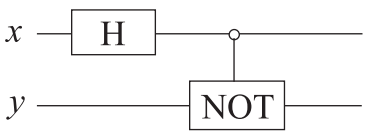
Как видно, выход не является произведением состояний $|\varphi\rangle\,|\psi\rangle$, за исключением тривиальных случаев $|\varphi\rangle = |0\rangle$ и $|\psi\rangle = |1\rangle$, так как в общем случае

$$|\varphi\rangle\,|\psi\rangle = a^2\,|00\rangle + ab\,|01\rangle + ab\,|10\rangle + b^2\,|11\rangle\,. \tag{7.29}$$

Другими словами такая цепь является цепью, создающей копию классического бита, но не копирует кубит. Общее свойство невозможности копирования кубита известно в квантовой теории информации как **теорема о неклонируемости кубита** (no-cloning theorem).

7.5 Состояния Белла

Рассмотрим более сложную квантовую цепь



$\Rightarrow |C_{xy}\rangle$ (7.30)

состоящую из однокубитового гейта Адамара и CNOT-гейта, и рассмотрим результат действия такой цепи на набор двухкубитовых состояний $|x, y\rangle$ вида: $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.

Например, при действии гейта Адамара на $|00\rangle$ на выходе будем иметь $(|0\rangle + |1\rangle)\,|0\rangle/\sqrt{2}$, а после действия гейта CNOT получим двухкубитовое состояние вида $(|00\rangle + |11\rangle)/\sqrt{2}$. Для всех четырех начальных состояний можно записать квантовый аналог таблицы истинности:

вход	выход
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|C_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|C_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|C_{10}\rangle$
$\|11\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|C_{11}\rangle$

(7.31)

Двухкубитовые состояния $|C_{ij}\rangle$, $i, j \in 0, 1$ называются **состояниями Белла** или **EPR-парами** (EPR≡Einstein-Podolsky-Rosen), которые обнаружили странные (необычные) свойства этих состояний. Сокращенно эти состояния можно записать в виде:

$$|C_{xy}\rangle \equiv \frac{|0y\rangle + (-1)^x\,|1\overline{y}\rangle}{\sqrt{2}}, \tag{7.32}$$

где $\overline{y} \equiv \neg y$.

7.6 Квантовый параллелизм

Квантовый параллелизм – это фундаментальное свойство квантовых вычислений. Данное свойство позволяет квантовым компьютерам вычислять функцию $f(x)$ для различных значений x одновременно.

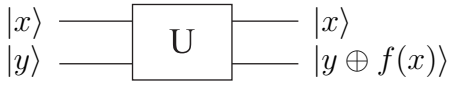
Для иллюстрации квантового параллелизма рассмотрим вычисление функции от битовой переменной x, результатом которой также является битовое значение

$$f(x) : \{0, 1\} \rightarrow \{0, 1\}. \tag{7.33}$$

Приемлемый способ вычисления этой функции на квантовом компьютере – это рассмотрение двухкубитового квантового компьютера, который оперирует с состоянием $|xy\rangle$. Используя соответствующую последовательность логических гейтов можно преобразовать исходное состояние $|xy\rangle$ в состояние $|x,\, y \oplus f(x)\rangle$. Здесь можно сказать, что x, y – регистры квантового компьютера. При этом первый регистр будем называть *регистром данных*, а второй – *регистром мишени*. Положим, что преобразование $|x, y\rangle \rightarrow |x,\, y \oplus f(x)\rangle$ осуществляется некоторым унитарным преобразованием U. В нашем случае мы можем рассматривать U как некий "черный ящик". Как следует из преобразования, если $y = 0$, то:

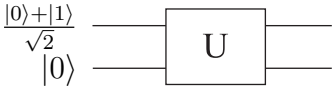
$$|x,\, 0\rangle \rightarrow |x,\, f(x)\rangle\,. \tag{7.34}$$

То есть в этом случае состояние второго кубита совпадает со значением вычисляемой функции $f(x)$.



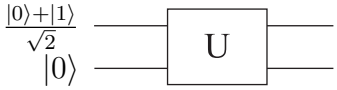
(7.35)

Рассмотрим квантовую цепь (7.35) которая действует на входные состояния вида



(7.36)

т.е. на регистр данных ($|\psi\rangle$) попадает суперпозиция $(|0\rangle + |1\rangle)/\sqrt{2}$, которая может быть создана действием гейта Адамара на кубит $|0\rangle$. В результате действия "черного ящика" U результирующее состояние будет иметь вид:



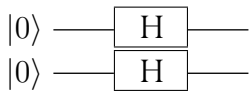
(7.37)

В данном удивительном результирующем состоянии различные члены содержат информацию как о значении $f(0)$, так и о значении $f(1)$! Фактически это соответствует вычислению функции $f(x)$ для двух значений x одновременно. Это свойство и обозначается в квантовых вычислениях как "квантовый параллелизм". В отличие от организации параллельных вычислений в классических компьютерах, когда технически создается несколько параллельных цепей, производящих вычисления одновременно в квантовом компьютере это осуществляется в одной цепи на суперпозиции состояний.

Данная процедура может быть легко обобщена для функции с произвольным числом битов путем введения преобразования Уолша-Адамара (Walsh-Hadamard), представляющее собой прямое произведение однокубитовых операторов Адамара:

$$\hat{W} \equiv \hat{H}_1 \otimes \hat{H}_2 \otimes \hat{H}_3 \otimes \cdots \otimes \hat{H}_n. \tag{7.38}$$

Данный оператор – есть n-штук гейтов Адамара, действующих параллельно на n-кубитов. Например, в случае $n = 2$ при действии на кубиты в начальном состоянии $|0\rangle$, получим



$$|\psi\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}. \tag{7.39}$$

В общем случае, результат действия гейта Адамара-Уолша на n-штук кубит, первоначально находящихся в состоянии $|0\rangle$ приводит к результату:

$$\hat{W}\,|0\rangle = \frac{1}{2^n} \sum_x |x\rangle\,, \tag{7.40}$$

где суммирование осуществляется по всем возможным состояниям x (см. пример при $n = 2$ (7.39)).

Такое преобразование Адамара-Уолша производит суперпозицию всех базисных состояний с равной амплитудой. Более того оно черезвычайно эффективно для построения суперпозиции 2^n состояний, используя при этом только n-гейтов.

Квантовые параллельные вычисления функции с n-битовым входом x и однобитовым выходом $f(x)$ могут быть построены следующим образом. Приготовим $n+1$-кубитовое состояние $|0\rangle$ на выходе. Применим преобразование Уолша-Адамара к первым n-кубитам, с последующим применением цепи U. В результате получим состояние

$$U\hat{W}^{(n)}\,|0\rangle \;\rightarrow\; \frac{1}{\sqrt{2^n}}\sum_x |x\rangle\,|f(x)\rangle\,. \tag{7.41}$$

В определенном смысле квантовый параллелизм способен вычислить возможные значения функции f одновременно для всех значений, хотя f вычисляется только один раз! Однако такой параллелизм оказывается не очень-то полезным.

Действительно, в нашем двухкубитовом примере измерение состояния даст только $|0,\,f(0)\rangle$ или $|1,\,f(1)\rangle$. Аналогично в общем случае, измерение состояния $\sum_x |x,\,f(x)\rangle$ может дать только $f(x)$ для одного значения x. Конечно и классический компьютер все это делает без труда. Квантовые вычисления должны приводить к результату более значительному, чем параллелизм. Необходимо иметь возможность извлекать информацию о более чем одном значении функции $f(x)$ из суперпозиции состояний подобно $\sum_x |x,\,f(x)\rangle$. Такая задача решается при построении специальных квантовых алгоритмов.

Ниже приводится пример действия гейта Уолша-Адамара на начальное n-кубитовое состояние $|0\rangle$. Если имеется произвольное n-кубитовое состояние $|x\rangle$ (например, $|x\rangle \equiv \underbrace{|01011\ldots\rangle}_{n}$), то

$$\hat{W}\,|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}\,|y\rangle\,,$$

где x, y— цепочки из 2^n состояний n-кубитов, а $x\cdot y$ обозначает их побитовое скалярное произведение по модулю 2, определяемое как

$$x\cdot y \equiv \sum_{n=0}^{2^n-1}(x_n \wedge y_n).$$